OFFICE OF
THE INSPECTOR GENERAL

U.S. NUCLEAR
REGULATORY COMMISSION

Use of the Internet at NRC

OIG-02-A-01 October 15, 2001

AUDIT REPORT

All publicly available OIG reports (including this report) are accessible through NRC's website at:
http://www.nrc.gov/NRC/OIG/index.html

October 15, 2001

MEMORANDUM TO: William D. Travers
Executive Director for Operations

FROM: Stephen D. Dingbaum**RA**\
Assistant Inspector General for Audits

SUBJECT: USE OF THE INTERNET AT NRC (OIG-02-A-01)

Attached is the Office of the Inspector General's audit report titled, *Use of the Internet at NRC*.

This report reflects the results of our review to determine whether NRC employees' use of the Internet is appropriate, and in compliance with NRC policy. Based on Internet activity over an eight day period in June 2001, at least 52 percent, and as much as 79 percent of employee Internet activity was for personal use. Some personal use, such as looking at sexually explicit web sites, was in direct violation of NRC policy. Personal use can also slow information transfer from the Internet, affecting the ability of others to use the Internet for business reasons. Because of the amount of personal use and the occurrence of prohibited activity, NRC needs to enforce its May 2001 information technology policy covering personal Internet usage.

At an exit conference held on October 3, 2001, NRC officials generally agreed with the report's findings and recommendations. While agency officials chose not to provide a formal, written response for inclusion in the report, they did provide editorial suggestions, which have been incorporated where appropriate.

If you have any questions, please contact Corenthis Kelley at 415-5977 or me at 415-5915.

Attachment: As stated

cc: John Craig, OEDO

R. McOsker, OCM/RAM
B. Torres, ACMUI
B. Garrick, ACNW
D. Powers, ACRS
J. Larkins, ACRS/ACNW
P. Bollwerk III, ASLBP
K. Cyr, OGC
J. Cordes, OCAA
S. Reiter, CIO
J. Funches, CFO
P. Rabideau, Deputy CFO
J. Dunn Lee, OIP
D. Rathbun, OCA
W. Beecher, OPA
A. Vietti-Cook, SECY
W. Kane, DEDR/OEDO
C. Paperiello, DEDMRS/OEDO
P. Norry, DEDM/OEDO
M. Springer, ADM
R. Borchardt, NRR
G. Caputo, OI
P. Bird, HR
I. Little, SBCR
M. Virgilio, NMSS
S. Collins, NRR
A. Thadani, RES
P. Lohaus, OSP
F. Congel, OE
M. Federline, NMSS
R. Zimmerman, RES
J. Johnson, NRR
H. Miller, RI
L. Reyes, RII
J. Dyer, RIII
E. Merschoff, RIV
OPA-RI
OPA-RII
OPA-RIII
OPA-RIV

EXECUTIVE SUMMARY

BACKGROUND

The Internet provides computer access to an ever-expanding storehouse of electronic information through the mass connection of networked computers. Use of the Internet offers tremendous capabilities to employees in terms of access to a wide variety of information sources relevant to their official duties. However, along with tremendous advantages, the Internet provides access to a wide variety of information that may not be consistent with business needs and may be harmful or inappropriate for the work place.

PURPOSE

The Office of the Inspector General conducted this review to determine whether Nuclear Regulatory Commission (NRC) employees' use of the Internet is appropriate and in compliance with NRC policy.

RESULTS IN BRIEF

Based on Internet activity over an eight-day period in June 2001, at least 52 percent and as much as 79 percent of employee Internet activity was for personal use. Some personal use, such as looking at sexually explicit web sites, was in direct violation of NRC policy. Visits to sexually explicit web sites are significant because the sites' contents may be offensive to others and could foster a hostile work environment, leading to potential legal liabilities for the agency. Personal use can also slow information transfer from the Internet, affecting the ability of others to use the Internet for business purposes. Because of the amount of personal use and the occurrence of prohibited activity, NRC needs to enforce and clarify its May 2001 information technology policy covering personal Internet usage.

RECOMMENDATIONS

This report makes five recommendations to the Executive Director for Operations to develop, issue, and communicate a revised Internet usage policy and to restrict prohibited use. Recommendations can be found at page 11 of this report.

AGENCY COMMENTS

At an exit conference held on October 3, 2001, NRC officials generally agreed with the report's findings and recommendations. While agency officials chose not to provide a formal, written response for inclusion in the report, they did provide editorial suggestions, which have been incorporated where appropriate.

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

I. BACKGROUND

In today's workplace, more and more companies are depending on the Internet to provide or enhance communication. While the Internet is fast and inexpensive, Internet usage can pose significant risks if it is not managed or is abused.

The various forms of Internet activity have become ingrained in most corporate cultures. Today, the Internet is used by roughly 90 million business workers in the United States (U.S.) (about two-thirds of all workers) and about 120 million workers outside the U.S. E-mail has replaced the telephone as the primary and preferred method of business communication for those with Internet access.

The Internet provides computer access to an ever-expanding storehouse of electronic information through the mass connection of networked computers. Use of the Internet offers tremendous capabilities to employees in terms of access to a wide variety of information sources relevant to their official duties. However, along with tremendous advantages, the Internet provides access to a wide variety of information that may not be consistent with business needs and may be harmful or inappropriate for the work place. Abuse, misuse, and overuse by employees can:

- in egregious cases, leave employers vulnerable to lawsuits (downloading of sexually explicit material has been viewed as creating a hostile work environment);

,

- introduce various security issues, such as the release of confidential, proprietary, or otherwise sensitive information, or a download of unlicenced software or viruses;

- cause a decline in employee productivity; and

- strain network resources.

To counter these risks, organizations can approach the issue from both behavioral and technological standpoints. Implementing a comprehensive Internet usage policy addresses the behavioral issues. Such a policy codifies usage guidelines and directives, designed to inform and educate employees about proper practices with regard to Internet activity. Organizations must also adopt technical measures, including:

- tools to monitor Internet activity to enforce policy and identify offenders;

- antivirus utilities to protect against malicious code at all potential points of infection;

- secure e-mail solutions to protect information traveling across the Internet; and

- archiving utilities and storage systems to ensure that messages are deleted or retained as appropriate.

A recent American Management Association survey found that more than three-quarters of major U.S. firms (77.7 percent) record and review employee communications and activities on the job, including Internet use. This figure has doubled since 1997. These firms monitor activity for a variety of reasons including (1) legal compliance, (2) legal liability, (3) performance review, (4) productivity measures, and (5) security concerns.

II. PURPOSE

The Office of the Inspector General (OIG) conducted this review to determine whether Nuclear Regulatory Commission (NRC) employees' use of the Internet is in compliance with policy. Appendix A provides details of the scope and methodology of this review.

III. FINDING

NRC NEEDS TO ENSURE COMPLIANCE WITH ITS INTERNET USAGE POLICY

Based on Internet activity from June 1- 8, 2001, at least 52 percent and as much as 79 percent of employee Internet activity is for personal use. Some personal use, such as looking at sexually explicit web sites, was in direct violation of NRC policy. Personal use can also slow information transfer from the Internet, affecting the ability of others to use the Internet for business purposes. Because of the amount of personal use and the occurrences of prohibited use, NRC needs to enforce its policy for personal Internet usage.

Employee Use of the Internet Is Mostly for Personal Reasons

The Federal Chief Information Officer Council issued Government-wide policy guidance on Internet usage in May 1999.[1] NRC's revised information technology policy, including Internet use, issued in May 2001,[2] closely follows this guidance. Under NRC's policy, personal Internet use is acceptable when it involves minimal or no additional expense to the Government, is performed on the employee's non-work time, does not interfere with NRC's mission or operation, does not violate the Standards of Ethical Conduct for Employees of

1 *Recommended Executive Branch Model Policy/Guidance on Limited Personal Use of Government Office Equipment Including Information Technology*, Federal Chief Information Officer Council, May 28, 1999.

2 NRC Management Directive 2.7, *Personal Use of Information Technology,* dated May 9, 2001.

the Executive Branch regulations, and is not otherwise prohibited by law. Prior to the May 2001 information technology policy, NRC restricted employees' use of the Internet to business only.

NRC maintains an Internet connection through an Internet service provider to serve the needs of its employees. Employee computers connected to an NRC network are always connected to the Internet. NRC then provides a single control point for all employee Internet use: a proxy server that is part of NRC's firewall system. All information from Internet sites accessed by NRC employees comes through the proxy server before being delivered to individual computers. Appendix B provides a diagram of NRC's firewall system. NRC's firewall system creates a log reflecting all of the Internet activity of employees. The log also records a number of pieces of information related to each Internet access.

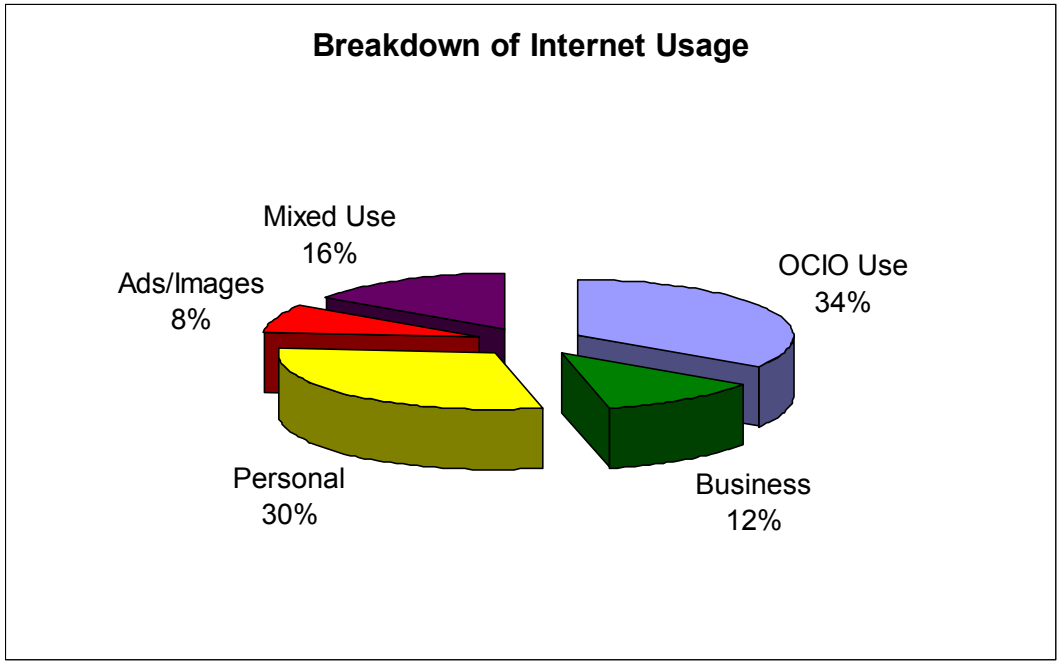
OIG reviewed employee[3] Internet use over an eight-day period in June 2001, a period shortly following issuance of NRC's revised policy. To analyze employee use of the Internet, OIG used data from NRC's firewall log that provided the amount of information transferred[4] through the proxy server. Internet activity was categorized as business or personal or other based on the material at the web site. In addition, some sites could have been used for either business or personal reasons (Mixed Use in this report). Examples are news sites and search engines.

The Office of the Chief Information Officer (OCIO) also routes a significant amount of information through the proxy server in monitoring network conditions throughout NRC's local and wide-area networks. And eight percent of the activity is the result of advertising and other unrelated images that are displayed when viewing web pages. The following chart shows a breakdown of Internet use at NRC.[5]

3 Employee use includes use of the Internet by NRC contractors. Contractors are not specifically covered by NRC's Internet usage policy.

4 This information transfer is referred to in this report as activity and indicates the actual number of bytes of information that were transferred to an employee's computer through the proxy server. Activity reflects the actual burden of Internet use on NRC's systems.

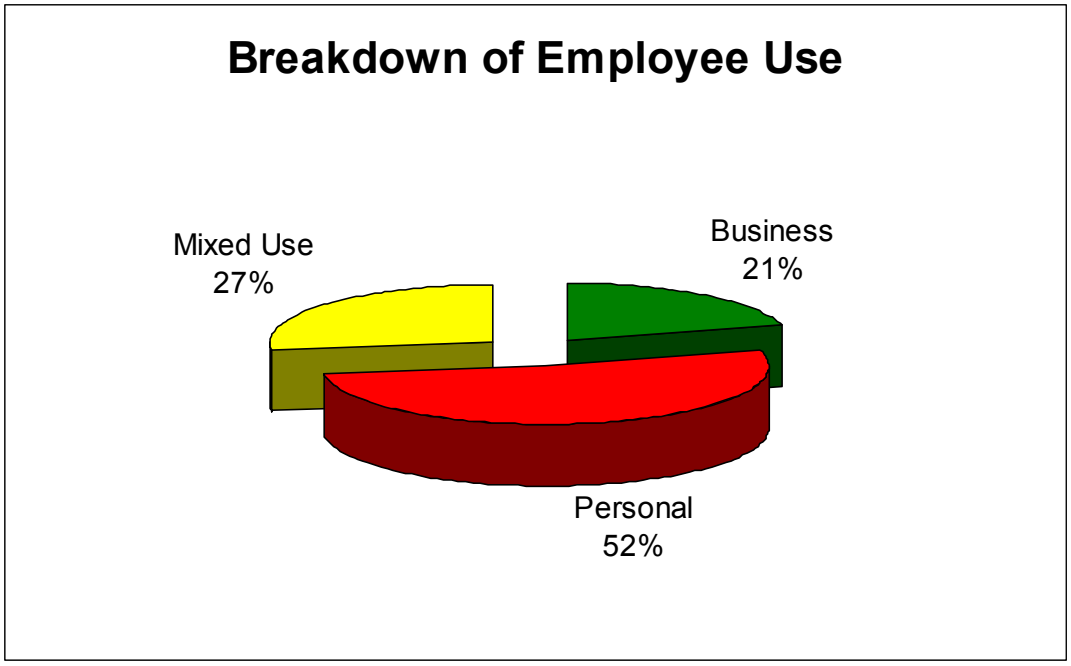
5 Results discussed in this report are based on analysis of a sample representing about 75 percent of all Internet activity.



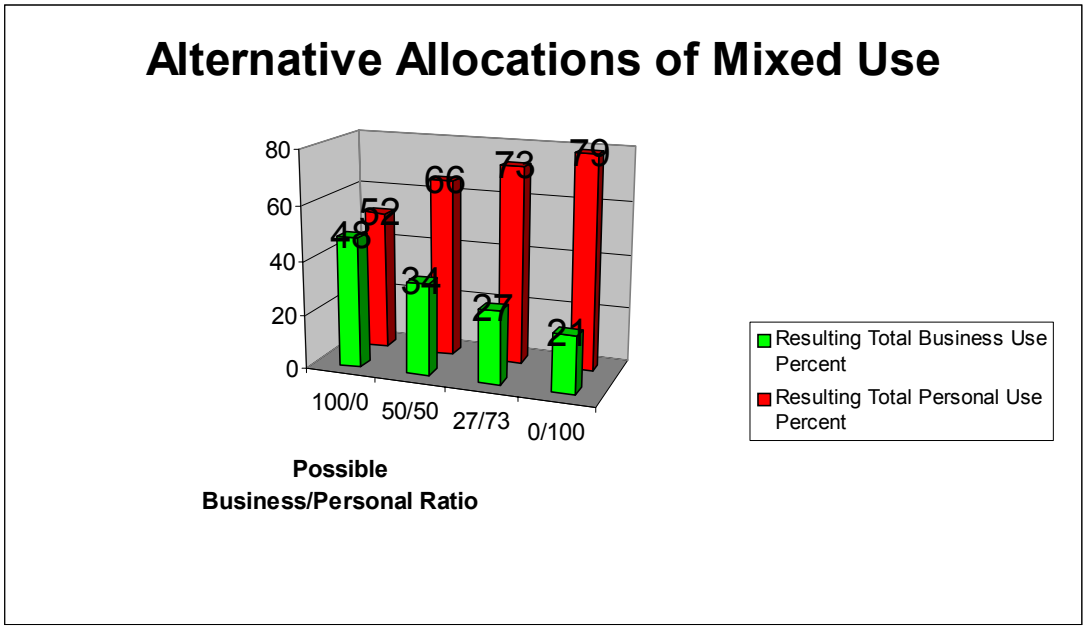
As the chart indicates, the two largest users of NRC's Internet system are OCIO, to monitor the status of its networks[6], and employees for personal reasons. The advertising and images loaded with Web pages are a large percentage of the activity coming through NRC's Internet connection.

6 OIG informed OCIO of these results and OCIO is currently evaluating how it can reroute this traffic to reduce the burden on the proxy server.

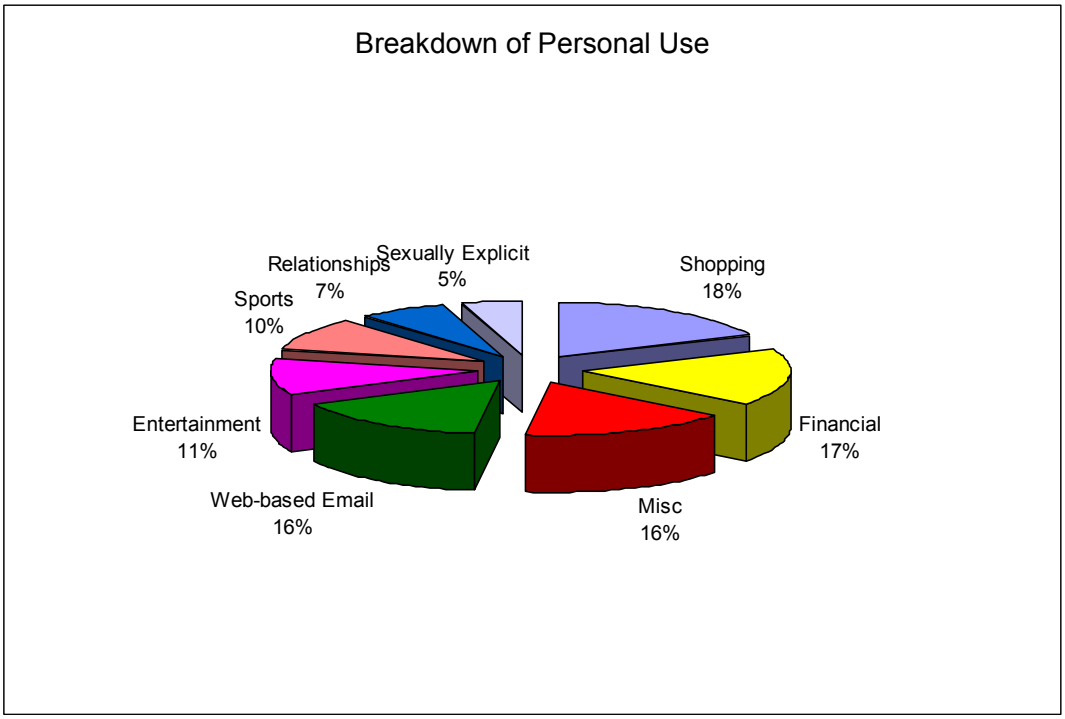
To obtain statistics solely on employee Internet usage, OIG eliminated the OCIO monitoring activity and Ads/Images from the analysis. Activity in those categories does not reflect the nature of sites accessed by employees. The following chart then shows how employees are using the Internet.



The Mixed Use category shown in the previous chart is dominated by employees accessing sites providing local and national news such as the Washington Post, CNN, and USA Today. Those sites were not placed in either the business or personal use category because OIG found no completely sound basis for doing so.[7] Such sites could be potentially used for either business or personal reasons. While OIG did not categorize these sites, the following chart provides the reader the results of allocating different percentages of Mixed Use activity to business or personal use. If the Mixed Use activity is eliminated, the ratio of business to personal activity is 27 percent to 73 percent. Allocating Mixed Use in this same ratio then results in no effect. As shown in this chart, at least 52 percent and as much as 79 percent of employee Internet activity was for personal use.



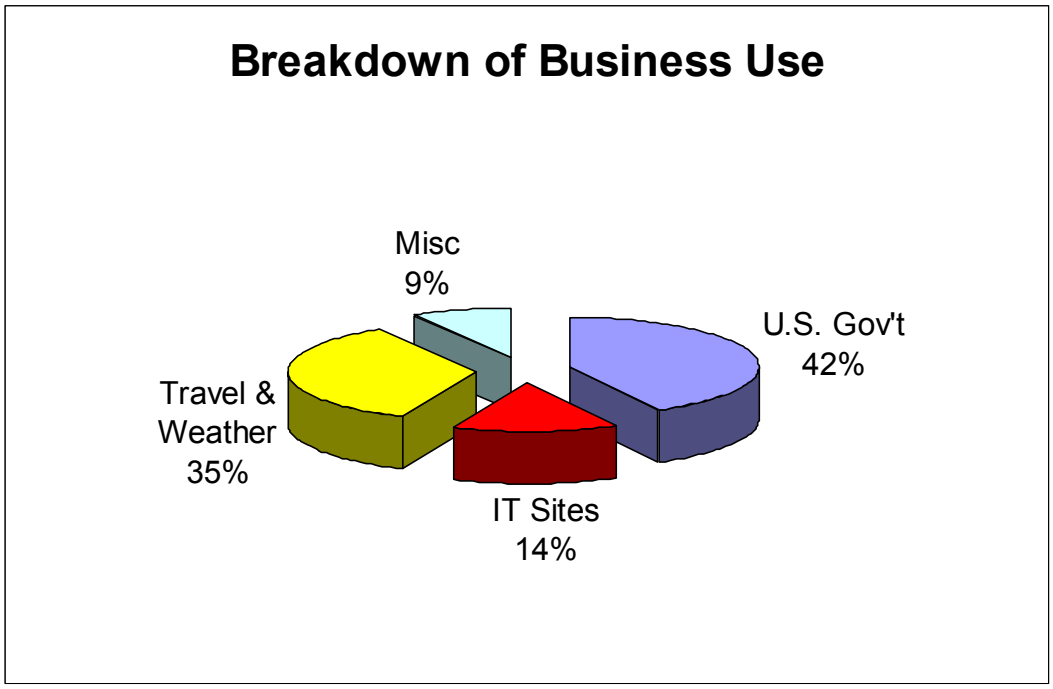
7 The information viewed by employees at each news and search engine site can be specifically determined and the activity categorized as business or personal. However, that requires examining tens or hundreds of thousands of web pages and was beyond OIG's resource capabilities.



A further breakdown of the 52 percent of Internet activity categorized above as personal use is shown in the above chart. As shown, employees accessed a wide variety of sites. In addition, a significant number of individuals, including contractors, abused the May 2001 usage policy. For example, more than 25 individuals used NRC's Internet connection and Government computers to access sexually explicit web sites.[8] In addition, a number of individuals accessed other sites potentially in violation of NRC policy, including gambling and hate sites. Visits to these types of web sites are significant because the sites' contents may be offensive to others and could foster a hostile work environment, leading to potential legal liabilities for the agency. Additionally, the risk of liability could increase without active enforcement of the agency's policy.

8 Based on the first week's results, review of prohibited activity was expanded to include information from May 21 through June 8, 2001. This prohibited activity was referred to OIG's investigative staff.

The following chart provides a breakdown of business use. OIG considered all travel and weather, and all IT sites as business.



The following table shows the ten sites with the most activity accessed for either business, personal, or a combination of personal and business reasons.

	Internet Address	Use	Category
1	www.washingtonpost.com	Mixed Use	news
2	www.cnn.com	Mixed Use	news
3	home.netscape.com	Mixed Use	news
4	www.sportingnews.com	Personal	sports
5	aolmail.aol.com	Personal	web-based e-mail
6	www.geocities.com	Mixed Use	news
7	www.usatoday.com	Mixed Use	news
8	trading.etrade.com	Personal	financial
9	Members.BlackPlanet.com	Personal	relationships
10	www.ebay.com	Personal	shopping

Personal use can also affect system performance because, if substantial, it can considerably slow information transfer from the Internet, affecting the ability of others to use the Internet for business purposes. An agency official stated that

an increase in Internet transactions put a significant load on the current Internet equipment and resulted in Internet access problems agencywide.[9] The official told OIG that the problem would, hopefully, be addressed by a contractor in the next fiscal year.

Additional Concerns

NRC does not monitor Internet usage and does not screen for all potentially harmful activity.[10] As a result, in addition to being able to access prohibited material, employees are able to download files from the Internet that NRC does not allow employees to obtain via e-mail. Without a policy to address potentially damaging Internet activity and a screening process to enforce that policy, the agency puts itself at risk for significant Internet-related losses.

OIG verified that some potentially harmful files can be downloaded via the Internet. For example, OIG downloaded a Visual Basic Script file[11] from a reliable Internet site.[12] OIG sent the same file into NRC's network e-mail system via the Internet. When sent via e-mail, the file was identified as potentially harmful and removed from the e-mail message. A warning generated by the e-mail system indicated the potentially damaging nature of the file. Allowing such files to be downloaded from Internet sites could allow employees to either intentionally or unintentionally download potentially harmful files.

Executable files are one of the primary sources for virus propagation.[13] In addition, users downloading unauthorized executable files may expose the agency to issues of legal liability if the software is unlicenced. NRC's Internet usage policy prohibits the downloading of executable files. However, NRC does not actively restrict such downloads, such as stopping them at the firewall. The following table provides examples of the executable files that NRC employees downloaded from the Internet during the period reviewed.

---

9 While NRC's connection to the Internet has sufficient capacity for its current load, internal configuration problems are resulting in poor performance during peak usage periods.

10 NRC officials told OIG they run a virus scan on Web-based e-mail and that the firewall system also filters certain types of content such as Java and ActiveX which are potentially malicious.

11 Visual Basic Script (VBS) is a programming language that can invoke any system function--including starting, using and shutting down other applications without user knowledge. VBS programs can be embedded in certain files and provide active content via the Internet.

12 The site was Microsoft. OIG first downloaded the file to a floppy disk and scanned it for harmful content.

13 An executable file is contrasted with a document or data file and is usually executed by double-clicking its icon or a shortcut on the desktop. The vast majority of known viruses infect executable files. Most infected files are transmitted via e-mail.

Compaq diagnostic software for WIN95/98
Flashplayer - enables display of certain animated material
WebShots screensaver
Acrobat Reader software for Palm computers
Microsoft Instant Messenger
AOL (America Online) Instant Messenger

AOL Instant Messenger was downloaded a number of times by NRC employees during the period reviewed, an activity prohibited by current policy if the software is unauthorized. Security and consulting firm @Stake has issued a security advisory warning against possible risks associated with AOL Instant Messenger. According to @Stake, a security weakness would allow an attacker, through e-mail or a malicious Web site, to remotely take control of a machine with AOL Instant Messenger installed; the program does not even have to be in use.

IV. SUMMARY

NRC employees are allowed to access information technology, including the Internet for personal purposes when that use is in accord with NRC's minimal use policy. Other than OCIO monitoring tools, use of the Internet is, for the most part, personal and is affecting system performance. In addition, prohibited activity is occurring. However, NRC does not currently monitor Internet activity.

Granting employees access to the Internet is an effective business tool. Misuse of the Internet, however, can diminish productivity and increase telecommunications demands. To minimize the misuse of the Internet, management must take actions to increase employee' awareness of the impact of misuse, monitor use, and block prohibited sites and activity. In addition, management must be proactive in establishing a policy that reflects all uses and their implications to both employees and contractors. Failure to do so leaves the agency vulnerable to threats posed by malicious files and vulnerable software, the download and use of unlicenced software, and the potential legal liability of such activities.

V. RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Initiate monitoring of Internet activity.

2. Review and clarify MD 2.7 to address Internet activity not currently covered, such as Visual Basic Script file type downloads.

3. Revise NRC Management Directives, as appropriate, to ensure NRC's Internet use policy covers persons other than NRC employees who use NRC computers to access the Internet.

4. Restrict prohibited Internet activity using software or other means.

5. Issue a Yellow Announcement, or other appropriate communication, advising employees and other affected users of the agency's revised policy and emphasizing that management will not tolerate prohibited activity.

VI. AGENCY COMMENTS

At an exit conference held on October 3, 2001, NRC officials generally agreed with the report's findings and recommendations. While agency officials chose not to provide a formal, written response for inclusion in the report, they did provide editorial suggestions, which have been incorporated where appropriate.

[Page intentionally left blank.]

SCOPE AND METHODOLOGY

The scope of this audit was generally limited to analysis and evaluation of the use of the Internet during eight days in June 2001. To perform this review and build a profile of employee usage, OIG obtained firewall logs from the agency for the period under review. OIG determined the amount of information transferred from each Web site using Microsoft Access and IDEA software. This information transfer (termed activity) indicates the actual number of bytes of information that were transferred to an employee's computer through the proxy server. Activity reflects the actual burden of Internet use on NRC's systems. OIG analyzed employee Internet usage by reviewing the 500 Web sites with the most activity. Those sites represented about 75 percent of all Internet activity for the period reviewed.

OIG trimmed each full Internet address shown in the firewall log to a base address and reviewed the material at that address to evaluate it's probable use. For example, the Internet address http://www.nrc.gov/NRC/WHATIS/directio.html would be evaluated based on the content at http://www.nrc.gov. Where the base address did not provide sufficient information about the content available at a Web page, OIG looked at the full address(es). The Internet activity reviewed represented use by about 2,950 NRC employees and contractors.

Based generally on the material at the main web page for each site accessed by employees, OIG determined whether use was business, personal, or a combination of personal and business use. OIG did not determine whether employees were spending inappropriate amounts of time using the Internet for personal reasons because firewall logs do not provide sufficient information to make such a determination.

OIG reviewed NRC's current Internet usage policy and the proposed policy from the Federal Chief Information Officer Council. OIG also met with NRC officials in the Offices of the Executive Director for Operations and the Chief Information Officer.

This audit was conducted from June through August 2001 in accordance with generally accepted Government auditing standards and included a review of management controls related to the objectives of the audit. The major contributors to this report were:

Corenthis Kelley, Team Leader
Robert Moody, Audit Manager
Beth Serepca, Audit Manager

[Page intentionally left blank.]

AGENCY DIAGRAM OF NRC'S FIREWALL